UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/708,757	03/24/2004	Marvin Shannon	lms-wb-2004-03-23	2756

36395 7590 10/03/2007

MARVIN SHANNON
3579 EAST FOOTHILL BLVD, #328
PASADENA, CA 91107

EXAMINER	
BELANI, KISHIN G	

ART UNIT	PAPER NUMBER
2143	

MAIL DATE	DELIVERY MODE
10/03/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

mn

Office Action Summary	Application No.	Applicant(s)	
	10/708,757	SHANNON ET AL.	
	Examiner	Art Unit	
	Kishin G. Belani	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 February 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Priority

Receipt is acknowledged of provisional applications submitted on 03/24/2003, 12/14/2003, 01/15/2004, and 03/03/2004 under 35 U.S.C. 119(e), which papers have been placed of record in the file.

Claim Objections

Claim 16 is objected to because of the following informalities:

On line 4 of claim 16, change "domains are derived" to – domains is derived –

Claim 18 is objected to because of the following informalities:

Claim 18 starts with superfluous characters "QuickMarkQuickMark". Please delete these characters from claim 18.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 12-14 are rejected under 35 U.S.C. 102(e) as being anticipated by **Kephart (US Patent Publication # 6,732,149 B1).**

Consider **claim 12,** Kephart shows and discloses an electronic communication system comprising interconnected entities for transmission and receipt of messages (Abstract that discloses a system for processing undesirable electronic messages received from a network; Fig. 2 that shows a spammer 200, interconnected to Users A, B and C of Company A via Mail Server 208; column 9, lines 39-52 that disclose transmission and receipt of email messages), the system comprising, in at least one of said entities, a subsystem for processing messages comprising:

a unit which identifies a set of characteristics of a message (Fig. 2, Extract Sig block 214 and spam email message 212; column 9, lines 53-64 that disclose the functionality of the Signature Extraction Engine 214 that identifies a set of characteristics of message 212);

a memory which stores the set of identified characteristics of messages in a plurality of bulk message envelopes, each bulk message envelope including a frequency index (Fig. 2, Sig. DB 216; column 9, lines 55-58 which disclose that any new signatures extracted from a spam message are stored in a Signature DB; column 14, lines 15-17 which disclose that an array of hash value (calculated from the extracted signatures) counts is kept, and each time a particular hash value is computed, the count for that value is incremented by 1, thereby disclosing a frequency index);

a unit which compares the set of identified characteristics of a message to the bulk message envelopes (Fig. 2, Extract Sig. block 214, User B and message 222; column 9, lines 58-64 which disclose that User B 218 and User C 220's messages 222 are scanned and the message's signature compared with the signatures stored in the Signature DB 216; instances of substantially similar messages are prevented from transmission to users' inboxes); and

if the identified characteristics are similar to a stored bulk message envelope, increasing the frequency index of the bulk message envelope in response (column 9, lines 0032-0038 that disclose identifying the same set of characteristics of a second message and comparing the set of identified characteristics of the second message to the first message to find instances of the substantially similar messages; column 11, lines 0046-0056 and lines 0064-0067 and column 12, lines 0001-0003; column 14, lines 15-17 which disclose that in case the first and second messages have similar characteristics, only the frequency count of the first message is incremented); and

if the identified characteristics are dissimilar to any stored bulk message envelope, causing the set of identified characteristics to be stored in the memory as an additional bulk message envelope (Fig. 4, processing blocks 405 and 416 which show that in the event the characteristics in the second message don't match those in the first message, a new cluster data is created for the second message; column 12, lines 29-38 disclose the same details; column 14, lines 15-17 in addition show that a frequency count is incremented by 1, which for a newly created cluster is initialized to zero).

Consider **claim 13,** Kephart shows and discloses a computer program embodied on a computer-readable medium and/or memory device for providing a subsystem for processing messages (claim 33; Abstract that discloses a system with computer programs for processing undesirable electronic messages received from a network; Fig. 2 that shows a spammer 200, interconnected to Users A, B and C of Company A via Mail Server 208; column 9, lines 39-52 that disclose transmission and receipt of email messages) comprising:

an identification segment for extracting a set of characteristics of a message (Fig. 2, Extract Sig block 214 and spam email message 212; column 9, lines 53-64 that disclose the functionality of the Signature Extraction Engine 214 that identifies a set of characteristics of message 212);

a storage segment for storing the set of identified characteristics of a message in a bulk message envelope, each bulk message envelope including a frequency index (Fig. 2, Sig. DB 216; column 9, lines 55-58 which disclose that any new signatures extracted from a spam message are stored in a Signature DB; column 14, lines 15-17 which disclose that an array of hash value (calculated from the extracted signatures) counts is kept, and each time a particular hash value is computed, the count for that value is incremented by 1, thereby disclosing a frequency index);

a comparison segment for comparing the set of identified characteristics of a message to the bulk message envelopes (Fig. 2, Extract Sig. block 214, User B and message 222; column 9, lines 58-64 which disclose that User B 218 and User C 220's messages 222 are scanned and the message's signature compared with the signatures stored in

the Signature DB 216; instances of substantially similar messages are prevented from transmission to users' inboxes); and

if the identified characteristics are similar to a stored bulk message envelope, increasing the frequency index of the bulk message envelope by a unitary increment (column 9, lines 0032-0038 that disclose identifying the same set of characteristics of a second message and comparing the set of identified characteristics of the second message to the first message to find instances of the substantially similar messages; column 11, lines 0046-0056 and lines 0064-0067 and column 12, lines 0001-0003; column 14, lines 15-17 which disclose that in case the first and second messages have similar characteristics, only the frequency count of the first message is incremented); and

if the identified characteristics are dissimilar to any stored bulk message envelope, causing the set of identified characteristics to be stored in the memory as an additional bulk message envelope having a frequency index with a unitary value (Fig. 4, processing blocks 405 and 416 which show that in the event the characteristics in the second message don't match those in the first message, a new cluster data is created for the second message; column 12, lines 29-38 disclose the same details; column 14, lines 15-17 in addition show that a frequency count is incremented by 1, which for a newly created cluster is initialized to zero).

Consider **claim 14,** Kephart shows and discloses an article of manufacture comprising a machine readable medium and/or memory device that provides

instructions that, if executed by a machine operatively connected to an electronic messaging system, will cause the machine to perform operations including:

identifying a set of characteristics of a first message (Fig. 2, Extract Sig block 214 and spam email message 212; column 9, lines 53-64 that disclose the functionality of the Signature Extraction Engine 214 that identifies a set of characteristics of message 212);

storing the set of identified characteristics of the first message in a first bulk message envelope, the first bulk message envelope including a frequency index (Fig. 2, Sig. DB 216; column 9, lines 55-58 which disclose that any new signatures extracted from a spam message are stored in a Signature DB; column 14, lines 15-17 which disclose that an array of hash value (calculated from the extracted signatures) counts is kept, and each time a particular hash value is computed, the count for that value is incremented by 1, thereby disclosing a frequency index);

identifying the same set of characteristics of a second message; comparing the set of identified characteristics of the second message to the first bulk message envelope (column 9, lines 0032-0038 that disclose identifying the same set of characteristics of a second message and comparing the set of identified characteristics of the second message to the first message to find instances of the substantially similar messages);

upon determining that the second message has characteristics similar to those of the first bulk message envelope, increasing the frequency index of the first bulk message envelope by a unitary value (Fig. 2, Extract Sig. block 214, User B and message 222; column 9, lines 58-64 which disclose that User B 218 and User C 220's messages 222

are scanned and the message's signature compared with the signatures stored in the Signature DB 216; instances of substantially similar messages are prevented from transmission to users' inboxes);

upon determining that the second message has characteristics dissimilar to those of the first bulk message envelope, storing the set of identified characteristics of the second message in a second bulk message envelope, the second bulk message envelope including a frequency index with a unitary value (Fig. 4, processing blocks 405 and 416 which show that in the event the characteristics in the second message don't match those in the first message, a new cluster data is created for the second message; column 12, lines 29-38 disclose the same details; column 14, lines 15-17 in addition show that a frequency count is incremented by 1, which for a newly created cluster is initialized to zero).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness
or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 1-11, 20, 21 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Kephart (US Patent Publication # 6,732,149 B1)** in view of **Quine et al. (US Patent Application Publication # 2003/0187942 A1).**

Consider **claim 1,** Kephart shows and discloses a method for processing digital messages on an electronic communication system, each message having a header and a body (Abstract that discloses a method for processing undesirable electronic messages from a network; Fig. 2 that shows a system for the method; column 5, lines

18-21 that disclose detecting and handling undesirable email messages (having a header and a body)), comprising:

a condensed representation of the message body produced by eliminating message content not perceptible in the normal display mode of the message and converting the perceptible message content to a standardized format characterized by limited degeneracy (Fig. 5, processing blocks 502 and 504; column 13, lines 0020-0028 which disclose a process of creating a condensed ("invariant") representation of the message body by eliminating message content not perceptible in the normal display mode of the message, and converting the perceptible message content to a standardized format characterized by limited degeneracy (generating signatures from sequences of characters that may be highly unlikely to be found in a typical message); column 12, lines 0044-0050 also disclose the same details);

generating a plurality of hash values which represents the converted content of the message body (column 14, lines 13-15 that disclose creating hash values for the identified sequences in the message body);

storing the set of identified characteristics of the first message in a first bulk message envelope, the first bulk message envelope including a frequency index (Fig. 2, block 216 that shows storing identified sequences in SIG DB; column 9, lines 55-58 disclose the same details; column 14, lines 15-17 which disclose that an array of hash value counts is kept, and each time a particular hash value is computed, the count for that value is incremented by 1, thereby disclosing a frequency index);

identifying the same set of characteristics of a second message (column 9, lines 0032-0038 that disclose identifying the same set of characteristics of a second message);

comparing the set of identified characteristics of the second message to the first bulk message envelope (Fig. 2, Extract Sig. block 214, User B and message 222; column 9, lines 58-64 which disclose that User B 218 and User C 220's messages 222 are scanned and the message's signature compared with the signatures stored in the Signature DB 216; instances of substantially similar messages are prevented from transmission to users' inboxes);

upon determining that the second message has characteristics dissimilar to those of the first bulk message envelope, storing the set of identified characteristics of the second message in a second bulk message envelope, the second bulk message envelope including a frequency index with a unitary value (Fig. 4, processing blocks 405 and 416 which show that in the event the characteristics in the second message don't match those in the first message, a new cluster data is created for the second message; column 12, lines 29-38 disclose the same details; column 14, lines 15-17 in addition show that a frequency count is incremented by 1, which for a newly created cluster is initialized to zero);

upon determining that the second message has characteristics similar to those of the first bulk message envelope, increasing the frequency index of the first bulk message envelope by a unitary increment (column 11, lines 0046-0056 and lines 0064-0067 and column 12, lines 0001-0003; column 14, lines 15-17 which disclose that in case the first

and second messages have similar characteristics, only the frequency count of the first message is incremented).

However, Kephart does not explicitly disclose identifying a set of characteristics of a first message, the set including addresses extracted from the header and body of the message.

In the same field of endeavor, Quine et al., disclose the claimed method, identifying a set of characteristics of a first message, the set including addresses extracted from the header and body of the message (paragraph 0013, lines 4-6 that disclose parsing a message to determine a sender address (located in the "From" field of the email header); paragraph 0019 that discloses comparing different elements in the body of a message and extracting a URL with web address).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to identify a set of characteristics of a first message, the set including addresses extracted from the header and body of the message, as taught by Quine et al., in the method of Kephart, so as to be able to distinguish a spam email from a legitimate email.

Consider **claim 2,** and **as it applies to claim 1 above,** Kephart, as modified by Quine et al., further shows and discloses the claimed method, comprising:
identifying the same set of characteristics of a third message (Fig. 6, message M2 and processing blocks 602 and 604 that apply to a third message (original and M1 being the

first two); column 13, lines 20-24 which disclose identifying the same set of characteristics of a third message that were determined for the first two messages); comparing the set of identified characteristics of the third message to the first and second bulk message envelopes (Fig. 6, processing blocks 606-612 and 616 that show comparison with a local signature database that includes the signatures of previously processed messages; column 15, lines 56-67 disclose the same details);
upon determining that the third message has characteristics similar to those of either the first or second bulk message envelopes, increasing the frequency index of the most similar bulk message envelope by a unitary increment (column 14, lines 15-17 that disclose incrementing frequency counter by 1 whenever an incoming message's characteristics are found to be similar to those of previously stored messages' characteristics);
upon determining that the third message has characteristics dissimilar to those of the first and second bulk message envelopes, storing the set of identified characteristics of the third message in a third bulk message envelope, the third bulk message envelope including a frequency index with a unitary value (Fig. 4, processing blocks 405 and 416 which show that in the event the characteristics in the incoming message don't match those in the previously processed message, a new cluster data is created for the incoming message; column 12, lines 29-38 disclose the same details; column 14, lines 15-17 in addition show that a frequency count is incremented by 1, which for a newly created cluster is initialized to zero).

Consider **claim 3,** and **as it applies to claim 1 above,** Kephart, as modified by Quine et al., further shows and discloses the claimed method, in which the step of identifying the characteristics of each message comprises:

transforming the message to a reduced format (Fig. 5, processing blocks 502 and 504; column 13, lines 0020-0028 which disclose a process of transforming the message to a reduced ("invariant") format by eliminating message content not perceptible in the normal display mode of the message, and converting the perceptible message content to a standardized format (generating signatures from sequences of characters that may be highly unlikely to be found in a typical message); column 12, lines 0044-0050 also disclose the same details);

processing the reduced message to derive a condensed representation of the reduced message (column 14, lines 13-15 that disclose creating hash values for the identified sequences in the message body).

Consider **claim 4,** and **as it applies to claim 3 above,** Kephart, as modified by Quine et al., further shows and discloses the claimed method, in which the condensed representation comprises plural hashes (column 14, lines 13-15 that disclose creating multiple hash values for the identified sequences in the message body).

Consider **claim 5,** and **as it applies to claim 3 above,** Kephart, as modified by Quine et al., further shows and discloses the claimed method, in which the step of transforming the body to a reduced format comprises eliminating non-communicative

information from the message (Fig. 5, processing blocks 502 and 504; column 13, lines 0020-0028 which disclose a process of transforming message body to a reduced format ("invariant" representation) that comprises eliminating non-communicative information (removal all non-alphanumeric characters) from the message; column 12, lines 0044-0050 also disclose the same details).

Consider **claim 6,** and **as it applies to claim 3 above,** Kephart, as modified by Quine et al., further shows and discloses the claimed method, in which the step of translating the body to a reduced format comprises conforming communicative information in the message to a standardized format characterized by limited redundancy (Fig. 5, processing blocks 502 and 504; column 12, lines 0044-0050 which disclose generating signatures from sequences of characters found in the message body, generating checksums for portions of the message or other compressed data strings making up a reduced message format, corresponding to conforming communicative information in the message to a standardized format characterized by limited redundancy).

Consider **claim 7,** and **as it applies to claim 3 above,** Kephart, as modified by Quine et al., further shows and discloses the claimed method, in which the step of translating the body to a reduced format comprises eliminating address information from the message (Fig. 5, processing blocks 502; column 13, lines 0020-0028 which disclose extracting signatures from sequences of characters found in the message body, thereby

disclosing elimination of address information from the message, which exists in the message header).

Consider **claim 8,** and **as it applies to claim 1 above,** Kephart, as modified by Quine et al., further shows and discloses the claimed method, in which a set of characteristics of each message comprises address data associated with the message (in Quine et al. reference, Fig. 3; paragraph 0013, lines 0004-0023 that disclose how the address data is used to differentiate normal email messages from spam emails, thereby disclosing that address data associated with the message represents a characteristics of each message).

Consider **claim 9,** and **as it applies to claim 8 above,** Kephart, as modified by Quine et al., further shows and discloses the claimed method, in which the address data comprises the purported originating address of the message (in Quine et al. reference, Fig. 3; paragraph 0013, lines 0004-0023 that disclose how the address data may or may not be purported originating address of the message, by examining the trace data; and if finding it suspicious, transmitting a request to sender for authentication; if the sender's address is not the purported originating address, the request will be undeliverable).

Consider **claim 10,** and **as it applies to claim 8 above,** Kephart, as modified by Quine et al., further shows and discloses the claimed method, in which the address data comprises one or more addresses included in the body of the message (in Quine et al.

reference, paragraph 0019 that discloses a URL link (web address) along with a misrepresented hyperlink text within the body of a message).

Consider **claim 11,** and **as it applies to claim 8 above,** Kephart, as modified by Quine et al., further shows and discloses the claimed method, in which the address data comprises one or more addresses through which the message has purportedly been relayed (in Quine et al. reference, Fig. 3, decision block 310 that checks for the validity of the address trace to determine one or more addresses through which the message has purportedly been relayed; paragraph 0013, lines 0004-0023 that disclose how the address data may or may not be purported originating address of the message, by examining the trace data; and if finding it suspicious, transmitting a request to sender for authentication; if the sender's address is not the purported originating address, the request will be undeliverable).

Consider **claim 20,** and **as it applies to claim 4 above,** Kephart, as modified by Quine et al., further shows and discloses the claimed method, in which these plural hashes may be exchanged by different organizations or users to detect messages seen by others, in an anonymous query manner that preserves the privacy of the original messages (in Kephart reference, Fig. 6; column 15, lines 28-33 that disclose a Local Signature Database D2 being used to compare the hash value of the scanned message with the hash block of each cluster that contains matching signature; column 16, lines 37-53 that disclose sharing of hashes by the local organization with the parent

organization where the Master Signature Database is located; since only hash and signature values are shared, the privacy of the original messages is preserved.

Consider **claim 21,** and **as it applies to claim 4 above,** Kephart, as modified by Quine et al., further shows and discloses the claimed method, in which the plural hashes may be found in an adaptive hashing manner (in Kephart reference, Fig. 6; column 15, lines 28-55 that disclose a Locality-preserving hash function to compute a HashBlock for the scanned message, by comparing with the HashBlocks of each cluster that contains one of the matching signatures found at step 606, and mathematically computing a similarity for each such cluster.

Consider **claim 23,** and **as it applies to claim 3 above,** Kephart, as modified by Quine et al., further shows and discloses the claimed method, in which the bulk message envelopes found from messages in one electronic communication space are used to compare and correlate with those derived from messages or data in another electronic communication space (in Kephart reference, Fig. 6; column 15, lines 28-33 that disclose a Local Signature Database D2 being used to compare the hash value of the scanned message with the hash block of each cluster that contains matching signature; column 16, lines 37-53 which disclose that if an undesirable message has been discovered locally, the Master Signature Database may be updated with information about the new instance of the undesirable message, thereby disclosing that bulk message envelopes found from messages in one electronic communication space

are used to compare and correlate with those derived from messages or data in another electronic communication space.

Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Kephart (US Patent Publication # 6,732,149 B1)** in view of **Quine et al. (US Patent Application Publication # 2003/0187942 A1)** and further in view of **Barchi (US Patent Publication # 6,507,866 B1).**

Consider **claim 15,** and **as it applies to claim 3 above,** Kephart, as modified by Quine et al., discloses the claimed method, except wherein a set of characteristics of a bulk message envelope include heuristic properties relating to the formatting or presentation of the data in the messages.

In the same field of endeavor, Barchi discloses that a set of characteristics of a bulk message envelope include heuristic properties relating to the formatting or presentation of the data in the messages (column 4, lines 24-28 under the heading "Message-Based Heuristic Filtering" which disclose that such filtering attempts to identify undesired e-mail by analyzing segments of the received e-mail message such as special content).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to identify a set of characteristics of a bulk message envelope using heuristic properties relating to the formatting or presentation of the data

in the messages, as taught by Barchi, in the method of Kephart, as modified by Quine et al., so as to be able to distinguish a spam email from a legitimate email.

Claims 16 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Kephart (US Patent Publication # 6,732,149 B1)** in view of **Quine et al. (US Patent Application Publication # 2003/0187942 A1)** and further in view of **Huang (US Patent Application Publication # 2003/0231207 A1).**

Consider **claim 16,** and **as it applies to claim 3 above,** Kephart, as modified by Quine et al., discloses the claimed method, except wherein from a set of bulk message envelopes thusly made, and using various characteristics of these, a real time black list (RBL) of spammer domains is derived.

In the same field of endeavor, Huang discloses a method wherein from a set of bulk message envelopes thusly made, and using various characteristics of these, a real time black list (RBL) of spammer domains is derived (Fig. 5, block 504; paragraph 0073, lines 1-5 that disclose a smart spam filter 500 which comprises a real-time blacklist (RBL) checker 504 for deriving a real time black list (RBL) of spammer domains).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to provide a method wherein from a set of bulk message envelopes thusly made, and using various characteristics of these, a real time black list (RBL) of spammer domains is derived, as taught by Huang, in the method of

Kephart, as modified by Quine et al., so as to be able to distinguish a spam email from a legitimate email.

Consider **claim 17,** and **as it applies to claim 16 above,** Kephart, as modified by Quine et al., discloses the claimed method, except wherein the RBL is applied against the current set of messages, possibly with a delay to detect and block current types of unwanted messages, or against a new set of messages, to block unwanted messages.

In the same field of endeavor, Huang discloses a method wherein the RBL is applied against the current set of messages, possibly with a delay to detect and block current types of unwanted messages, or against a new set of messages, to block unwanted messages (paragraphs 0079, 0086, 0087 and 0095 that disclose a process of scoring incoming message as spam, e.g. if the message header comprises IP addresses in the RBL, a score of 50 is added to the total spam score. If the total spam score from the Advanced Raw Mode match is high enough, the IP addresses used in the header can be submitted to the RBL automatically; once the RBL is populated with sufficient IP addresses of known spammers, it may be used against the current set of messages, possibly with a delay to detect and block current types of unwanted messages, or against a new set of messages, to block unwanted messages).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to provide a method wherein the RBL is applied against the current set of messages, possibly with a delay to detect and block current

types of unwanted messages, or against a new set of messages, to block unwanted messages, as taught by Huang, in the method of Kephart, as modified by Quine et al., so as to be able to distinguish a spam email from a legitimate email.

Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Kephart (US Patent Publication # 6,732,149 B1)** in view of **Quine et al. (US Patent Application Publication # 2003/0187942 A1)** and further in view of **Huang (US Patent Application Publication # 2003/0231207 A1)** and further in view of **Engberg (US Patent Application Publication # 2003/0158960 A1).**

Consider **claim 18,** and **as it applies to claim 16 above,** Kephart, as modified by Quine et al. and Huang, discloses the claimed method, except wherein the RBL is used by various routing services or gateways or relay machines to block communications with entries in the RBL.

In the same field of endeavor, Engberg discloses a method wherein the RBL is used by various routing services or gateways or relay machines to block communications with entries in the RBL (Abstract and paragraph 0018 which disclose that through user controlled communication rules, including an access control filter (corresponding to RBL) and a dynamic routing service, the individual is in control of communication; Fig. 5, that shows a TP (Trusted Party) offering a routing service; paragraphs 0176 and 0177 that disclose TPs using blacklist to block communications with entries in the RBL).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to provide a method wherein the RBL is used by various routing services or gateways or relay machines to block communications with entries in the RBL, as taught by Engberg, in the method of Kephart, as modified by Quine et al. and Huang, so as to be able to enforce anti-spam requirements/desires of their (TPs) users.

Claims 19 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Kephart (US Patent Publication # 6,732,149 B1)** in view of **Quine et al. (US Patent Application Publication # 2003/0187942 A1)** and further in view of **Rounthwaite et al. (US Patent Publication # 7,219,148 B2).**

Consider **claim 19,** and **as it applies to claim 3 above,** Kephart, as modified by Quine et al., discloses the claimed method, except wherein the subsets of the bulk message envelopes are chosen, to which further filtering is applied; where the filtering might include Bayesian, neural network or other techniques, some of which are possibly dependent on human languages; where the subsets may be derived using various values of the bulk message envelopes, including, but not limited to, the frequency of each envelope.

In the same field of endeavor, Rounthwaite et al. disclose a method wherein the subsets of the bulk message envelopes are chosen, to which further filtering is applied (column 5, lines 66-67 and column 6, lines 1-3 that disclose classifying (applying

filtering to) a subset of the incoming messages (denoted as IM") as spam or not spam); where the filtering might include Bayesian, neural network or other techniques, some of which are possibly dependent on human languages (column 6, lines 7-13 which disclose employing machine learning techniques such as neural networks, SVMs, or Bayesian network; column 2, lines 46-49 which disclose users, identified as spam fighters, tasked with voting on whether a selection of incoming messages is either legitimate mail or junk mail, thereby disclosing human language dependent filtering technique);

where the subsets may be derived using various values of the bulk message envelopes, including, but not limited to, the frequency of each envelope (column 2, lines 55-62 which disclose that for each selected message, message properties, message classification, message content summaries, or statistical data (including frequency) related to any of the above, are used to generate sets of training data for machine learning systems).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to provide a method wherein the subsets of the bulk message envelopes are chosen, to which further filtering is applied; where the filtering might include Bayesian, neural network or other techniques, some of which are possibly dependent on human languages; where the subsets may be derived using various values of the bulk message envelopes, including, but not limited to, the frequency of each envelope, as taught by Rounthwaite et al., in the method of Kephart, as modified by Quine et al., so as to provide more effective filtering means for eliminating junk

e-mail.

Consider **claim 22,** and **as it applies to claim 3 above,** Kephart, as modified by Quine et al., discloses the claimed method, except wherein a user can maintain a "gray list" of desired bulk message senders, and the user's message provider uses claim 3 to find bulk messages addressed to the user, and from these bulk messages, forwards only those from senders on the gray list, to the user, where the determination of the sender of a message may involve examining the contents of a message, in addition to examining the purported sender field and other entries in the header.

In the same field of endeavor, Rounthwaite et al. disclose a method wherein a user can maintain a "gray list" of desired bulk message senders, and the user's message provider uses claim 3 to find bulk messages addressed to the user, and from these bulk messages, forwards only those from senders on the gray list, to the user, where the determination of the sender of a message may involve examining the contents of a message, in addition to examining the purported sender field and other entries in the header (column 7, lines 47-51 and 56-58 which disclose an additional (besides "spam" or "not spam" button for classifying a message) button such as a "solicited commercial email" button that can be provided based on the user's desire, thereby disclosing a user's "gray list" of desired bulk message senders).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to provide means for a user to maintain a "gray list" of desired bulk message senders, and the user's message provider using claim 3 to find

bulk messages addressed to the user, and from these bulk messages, forwarding only those from senders on the gray list, to the user, where the determination of the sender of a message may involve examining the contents of a message, in addition to examining the purported sender field and other entries in the header, as taught by Rounthwaite et al., in the method of Kephart, as modified by Quine et al., so as to provide additional options to users who would like bulk commercial type messages sent to them, instead of being blocked as spam.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

US Patent Application Publication 2005/0015456 A1; by Martinson, JR.;

filed 8/29/2003

Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Art Unit: 2143

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Kishin G. Belani whose telephone number is (571) 270-1768. The Examiner can normally be reached on Monday-Thursday from 6:30 am to 5:00 pm.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, David Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free) or 703-305-3028.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist/customer service whose telephone number is (571) 272-0800.

Kishin G. Belani

K.G.B./kgb

September 24, 2007

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100